AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Silver/Black Samsung Model A1533; Black Samsung Model SM-A600AZ; Black/Silver Apple iPhone Model A1688 red case; Black/Silver Apple iPhone Model A1688 brown case

Case No. **3:20-mj-002**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attchment A (incorporated by reference).

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2113(a)	Bank Robbery
18 U.S.C. § 924(c)(1)(A)	Using firearms during and in relation to crimes of violence

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 180 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Rafael Vences, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 1-6-20

Judge's signature

City and state: Galveston, Texas

Hon. Andrew M. Edison, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION

In the matter of the search of information associated with Silver/Black Samsung Model A1533; Black Samsung Model SM-A600AZ; Black/Silver Apple iPhone Model A1688 red case; Black/Silver Apple iPhone Model A1688 brown case	Case No. **3:20-mj-002**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, **Rafael Vences**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following electronic devices (collectively, the "**Target Devices**"), which are currently in the possession of the FBI, and the extraction from that property of electronically stored information described in Attachment B.

a. One silver and black Samsung (Model A1533) bearing IMEI 355370100594678 photographed in Attachment A, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 1**");

b. One black Samsung (Model SM-A600AZ) bearing IMEI 352065100614970 photographed in Attachment A, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 2**");

c. One black and silver Apple iPhone S (Model A1688, red case) photographed in Attachment A, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 3**");

d. One black and silver Apple iPhone S (Model A1688 brown case) photographed in Attachment A, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 4**").

2. I am a Special Agent with the **Federal Bureau of Investigation (FBI)**, and have been since **March 25, 2012**. Affiant received nineteen (19) weeks of training in criminal investigations and related legal matters at the FBI Training Academy in Quantico, Virginia. Affiant has received courses of instruction from the FBI relating to investigative techniques utilized in violent crime and financial investigations. Affiant has conducted investigations involving the interception of wire communications, and the approval of location based search warrants involving cellular devices. Affiant has participated in and conducted investigations which have resulted in the arrests of individuals who have committed bank robbery against financial institutions insured by the Federal Deposit Insurance Corporation (FDIC).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the information contained herein, there is probable cause to believe that the **Target Devices** contain evidence, fruits, and instrumentalities of the crimes of violations of Bank Robbery under 18 U.S.C. § 2113(a) and using firearms during and in relation to crimes of violence, under 18 U.S.C. § 924(c)(1)(A). The applied-for warrant would authorize the forensic examination of the **Target Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

5. The United States is investigating the robbery of the First State Bank of Louise, a financial institution insured by the FDIC, which took place on September 12, 2019. The investigation concerns possible violations of, Bank Robbery under 18 U.S.C. § 2113(a) and using firearms during and in relation to crimes of violence, under 18 U.S.C. § 924(c)(1)(A).

6. At approximately 11:22AM on September 12, 2019 two (2) unidentified subjects (UNSUBS) disguised with face coverings entered the front door of the First State Bank of Louise located at 505 E. Boling Highway, Wharton, Texas. The two (2) UNSUBS brandished semi-automatic pistols which they pointed at bank employees while making oral demands.

7. The UNSUBS made their way behind the teller counters and gained access to the money inside some of the teller tills. The UNSUBS then had one of the tellers open the bank vault. One of the UNSUBS emptied all the cash contained in the vault into a bag. Shortly after emptying the cash from the bank's vault the two (2) UNSUBS exited the bank from the front door at approximately 11:25AM. The reported loss from the First State Bank of Louise was approximately two-hundred-seventy-four-thousand-three-hundred-eighty-seven dollars ($274,387). First State of Louise bank records provided to Affiant indicated that five (5) bait bills had been taken by the UBNSUBS. The bait bill's serial numbers were provided to Affiant and recorded by Affiant.

8. During witness interviews, bank employees who were in the bank at the time of the robbery described the UNSUBS as black males. Subsequently, Wharton Police Department (WPD) detectives were able to obtain video surveillance footage from an adjacent business which captured video of the UNSUBS prior to and after the bank robbery. The video

surveillance system captured the UNSUBS without any facial covering. The WPD posted video stills of the unmasked UNSUBS on the WPD Facebook page.

9. Later that same day, Affiant was notified of the bank robbery and made contact with WPD investigators regarding the robbery which had taken place earlier. WPD detectives directed Affiant to their WPD public Facebook page where the video stills of the UNSUBS were posted. After navigating to the WPD Facebook page Affiant immediately recognized the UNSUBS as Tony Wayne **MITCHELL (MITCHELL)** and Leedward Demon **HOPKINS (HOPKINS). MITCHELL** and **HOPKINS** were suspects in multiple other bank robberies being investigated by Affiant.

10. Further, Affiant received a telephone call from a confidential human source (CHS), hereinafter referred to as "CS-1," regarding the bank robbery which had taken place in Wharton, Texas. CS-1 indicated that he/she had reviewed the WPD Facebook page and saw that video surveillance photos of **MITCHELL** and **HOPKINS** were posted as unidentified suspects in a bank robbery in Wharton, Texas. CS-1 stated to Affiant that he/she was absolutely sure the persons in the photos were **MITCHELL** and **HOPKINS.**

11. Affiant contacted WPD detectives and provided the detectives the identifiers and photos of **MITCHELL** and **HOPKINS.** Subsequently, WPD detectives obtained arrest warrants for **MITCHELL** and **HOPKINS.**

12. Later, on the evening of September 12, 2019 law enforcement officers from the Houston Police Department (HPD) setup a physical surveillance of **MITCHELL's** last know residence located at 9007 Alcott Drive, Houston, Texas. While conducting surveillance HPD officers observed a black male fitting the description of **MITCHELL** exited the residence located at 9007 Alcott and entered a white Infinity sedan which bore Texas License Plate No.

GJL 7436. HPD officers noticed the Infinity had an expired registration sticker and the vehicle failed to stop at the stop sign located at the intersection of Alcott and Hollister streets. HPD officers effected a traffic stop on the white Infinity which resulted in a pursuit and crash near 12100 Hempstead Road.

13. The driver of the vehicle was identified as Mikell **PHILLIPS**. Inside the Infinity HPD officers located amongst other things approximately one-point-seven (1.7) kilograms of ecstasy pills, ninety-six-thousand-one-hundred-fifty dollars in United States (US) currency ($96,150), and the **Target Devices**. **PHILLIPS** was also found to have nine (9) outstanding felony warrants and one (1) misdemeanor warrant. **PHILLIPS** was taken into custody and charged with "Possession with Intent to Distribute a Controlled Substance," and "Evading in a Motor Vehicle."

14. HPD detectives reviewed the US currency seized from **PHILLIPS** and determined that the currency was bundled with bands. HPD shared this information with the WPD and WPD detectives determined the bands were similar to the money bands used by the First State Bank of Louise in Wharton, Texas. On November 20, 2019 Affiant had the US currency seized from **PHILLIPS** scanned and re-counted using a Cummins Allison JetScan model iFX100 money counting machine and currency scanner. Later that same day Affiant used the scanned currency images to perform a search for the serial numbers of the bait bills discussed in paragraph seven (7) above. Affiant's search identified all five (5) bait bills in the US currency seized from **PHILLIPS**.

15. Based on my training, experience, and knowledge of the facts and circumstances of this investigation Affiant logically concluded that the US currency possessed by **PHILLIPS** was the same US currency taken by **MITCHELL** and **HOPKINS** from the First State Bank of

Louise on September 12, 2019. A search of **MITCHELL**'s social media (Facebook) page indicated **MITCHELL** is "Facebook friends" with **PHILLIPS**. Further, CS-1 indicated to Affiant that **MITCHELL** and **PHILLIPS** are friends. This information was corroborated by **MITCHELL** and **HOPKINS'** friend Tiffany **GUILLORY** whom Affiant interviewed on September 13, 2019. **GUILLORY** indicated that **PHILLIPS** was from Dallas, Texas and a close friend of **MITCHELL**.

16. Based on my training, experience, and knowledge of the facts and circumstances of this investigation, and Affiant's review of video surveillance footage on the day of the robbery of the First State Bank of Louise, Affiant concluded that **MITCHELL** and **HOPKINS** were dropped off and picked up during the robbery by a yet unidentified co-conspirator. Affiant further concluded that a forensic examination of the **Target Devices** may contain evidence assisting Affiant in the identification of the unidentified co-conspirator.

FACTS ABOUT CELLULAR TELEPHONES

17. Based on my training and experience and the training and experience of law enforcement personnel who routinely handle this type of equipment, I understand that the **Target Devices** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when it first came into the law enforcement's possession..

18. Based on my training, experience, and information provided to me by other law enforcement personnel, I am aware that individuals carry out, communicate about, and store records regarding their daily activities on equipment like the **Target Devices**. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, text messages, and other forms of phone or internet-based messages; scheduling activities; keeping a calendar of

activities; arranging travel; purchasing items; searching for information on the internet; accessing personal accounts including banking information; paying for items; and creating and storing images and videos of their movements and activities.

19. Based on my training, experience, and information provided to me by other law enforcement personnel, I am aware that individuals involved in the planning and execution of armed robberies communicate with each other through the use of cellular telephones like the **Target Devices**. Additionally, I am also aware that individuals involved in the planning and execution of armed robberies communicate using social media networking sites like Facebook, Snapchat, WhatsApp, etc. which can be accessed through cellular telephones like the **Target Devices**.

20. I also know that many smartphones like the **Target Devices** (which are included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Based on my training, experience, and information provided to me by other law enforcement personnel, I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.

21. Through my training and experience, I know that oftentimes individuals engaged in criminal activity will discard and/or replace old phones in an attempt to evade detection by law enforcement or to prevent law enforcement from seizing digital evidence from a particular

device. However, although an actual device may be switched by a suspect, information contained in and/or associated with the previous device can be transferred to the new device. This transfer of information usually occurs, amongst other reasons, because individuals generally continue to use the same Apple ID / Android ID (accounts designed to store a user's information) when switching between physical devices.

22. Based on my training, experience, and information provided to me by other law enforcement personnel, I know that data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer the data from their old device to a new one.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of

operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

CONCLUSION

23. Based on the information described above, I have probable cause to believe that evidence, fruits, and instrumentalities of the crimes of Bank Robbery under 18 U.S.C. § 2113(a) and using firearms during and in relation to crimes of violence, under 18 U.S.C. § 924(c)(1)(A), as further described in Attachment B, are contained within the equipment described in Attachment A.

Respectfully submitted,

Rafael Vences
Special Agent
Federal Bureau of Investigation

Subscribed and sworn via telephone on Jan 6, ~~2019~~ 2020

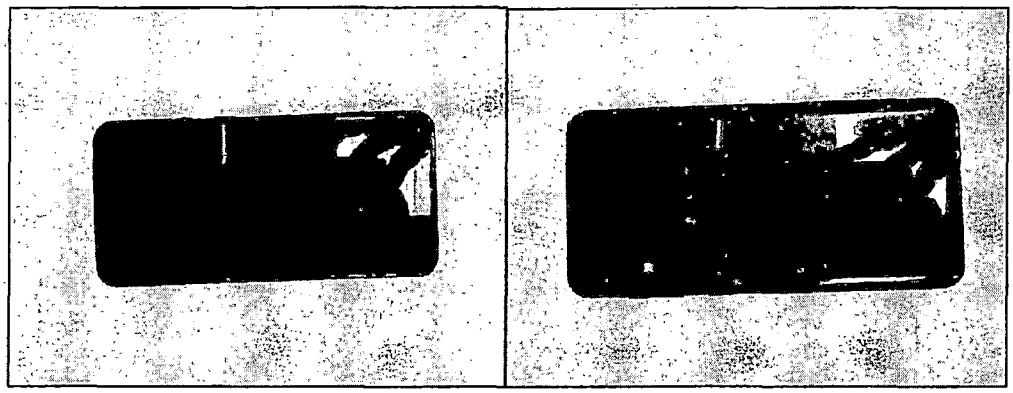
ANDREW M. EDISON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

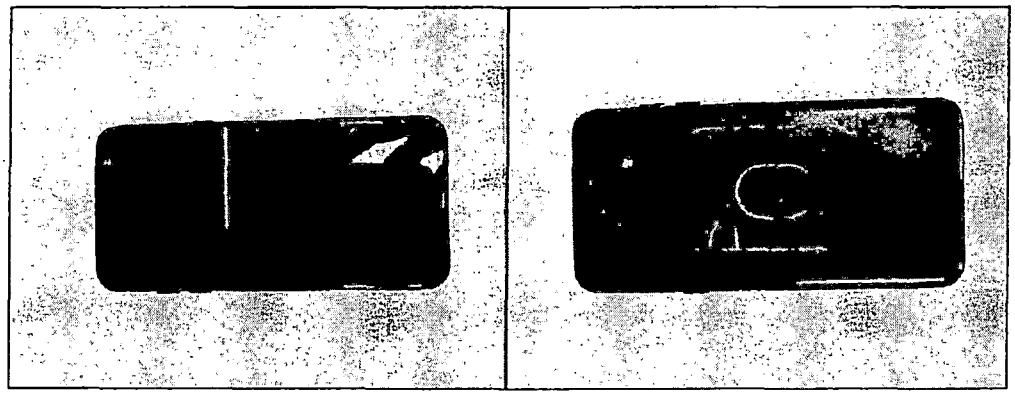
Description of Equipment to be Searched

The equipment to be searched consists of the following:

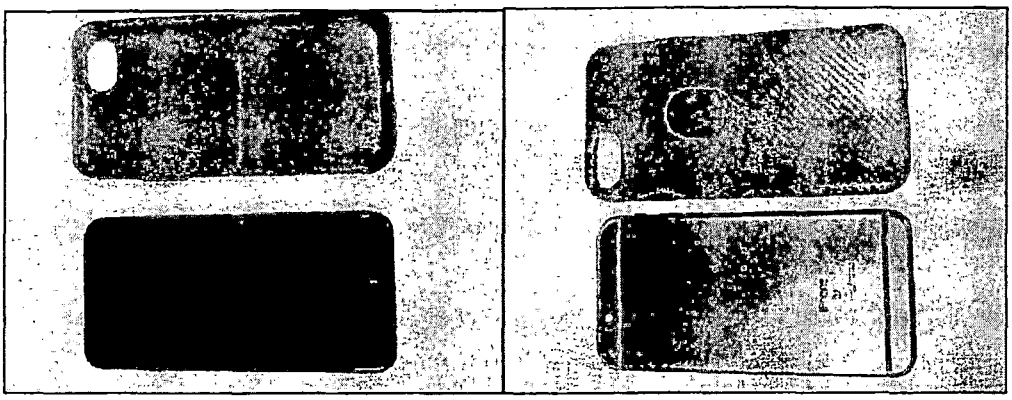
- One silver and black Samsung (Model A1533) bearing IMEI 355370100594678 photograph below, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 1**");



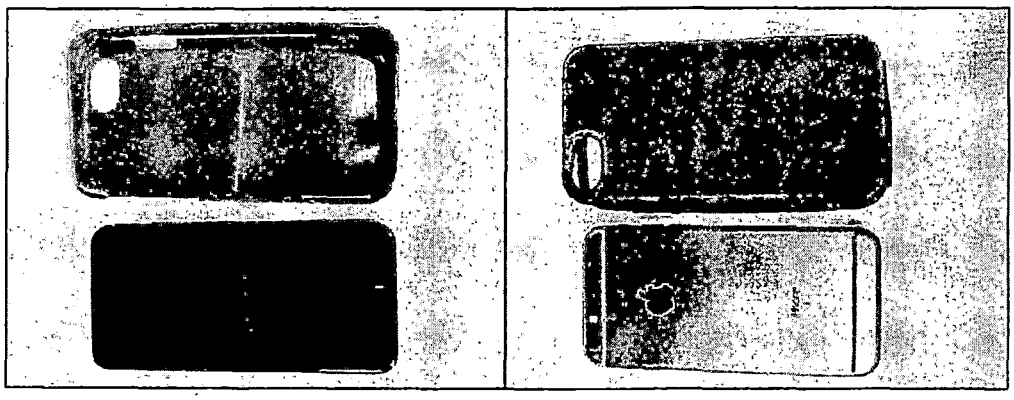
- One black Samsung (Model SM-A600AZ) bearing IMEI 352065100614970 photographed below, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 2**")



- One black and silver Apple iPhone S (Model A1688, with red case) photograph below, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX ("**Target Device 3**");



- One black and silver Apple iPhone S (Model A1688 with brown case) photograph below, seized on September 12, 2019 from Mikell PHILLIPS at 12100 Hempstead Road in Houston, TX (**"Target Device 4"**).



The Target Devices are located at the Federal Bureau of Investigation, 600 Gulf Freeway, Suite 211 Texas City, Texas.

ATTACHMENT B

Description of Information or Items to Be Seized

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2113(a) and 18 U.S.C. § 924(c)(1)(A), including those related to:

A. Evidence of who used, owned, or controlled the equipment;

B. The identities and aliases of individuals whom participated in armed robbery;

C. The locations where planning and/or actual robberies occurred;

D. The locations where evidence or other items related to armed robbery were discarded;

E. The methods of communication between participants of the armed robberies, including the telephone numbers, messaging applications, and social media accounts used by the individuals;

F. The substance of communications regarding the planning, execution, and/or discussion of robberies

G. The substance of communications regarding the acquisition, disposal, and/or discussion of clothing, firearms, and other items intended to be used before, during, or after the commission of armed robberies;

H. The substance of communications regarding firearms and/or ammunition;

I. The substance of communications regarding money or other items acquired during robberies;

J. Photographs of items or information related to the planning, execution, or discussions related to armed robbery;

K. The relationship between the users of the Target Devices and other identified co-conspirators;

L. The identity, location, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

M. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

N. Evidence of the attachment of other hardware or storage media;

O. Evidence of counter-forensic programs and associated data that are designed to eliminate data;

P. Evidence of the times the equipment was used;

Q. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

R. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media; and

S. Records relating to the ownership, occupancy, or use of the location from which the equipment was obtained by law enforcement investigators.

II. Serial numbers and any electronic identifiers that serve to identify the equipment.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or

thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.